AMENDMENTS TO CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently Amended) A system for securing input of non-PIN data using a numeric keypad of a PINpad terminal, said PINpad terminal comprising:

a numeric keypad including a plurality of numeric keys through which data is input, processing of said data being initiated by at least one prompt table file in response to display of prompts listed in the prompt table;

a memory for storing said at least one prompt table file;

a display for displaying said prompts;

~~a~~ wherein said dynamic prompt table file is arranged to permit numeric keys on the keypad to be used for entry of non-PIN data if and only if an appropriate prompt has been, and continues to be, displayed at the time of data entry; and

said system further comprises a file authentication arrangement for authenticating said dynamic prompt table file upon loading of the dynamic prompt table file in the terminal.

2. (Original) A system as claimed in claim 1, wherein said file authentication arrangement includes a private key and a corresponding public key certificate containing information necessary to authenticate the prompt table file.

3. (Original) A system as claimed in claim 2, wherein said private key is stored on a smartcard and is only accessible by a secure processor embedded in the smartcard.

4. (Original) A system as claimed in claim 2, further comprising a file signing tool for digitally signing said clear file, said file signing too including a smartcard reader, and wherein all digital

signing operations requiring access to said private key are carried out by a secure processor embedded in a smartcard inserted into said smartcard reader.

5. (Original) A system as claimed in claim 2, wherein said smartcard further has stored thereon a signer certificate for authenticating said digital signature, said signer certificate being authenticated by a sponsor certificate pre-installed in the terminal.

6. (Currently Amended) A method of securing input of non-PIN data using a numeric keypad of a PINpad terminal, said PINpad terminal comprising:

a numeric keypad including a plurality of numeric keys through which data is input, processing of said data being initiated by at least one prompt table file in response to display of prompts listed in the prompt table;

a memory for storing said at least one prompt table file;

a display for displaying said prompts,

said method comprising the steps of:

~~providing a dynamic prompt table file arranged to permit~~ permitting said numeric keys on the keypad to be used for entry of non-PIN data if and only if an appropriate prompt has been, and continues to be, displayed at the time of data entry; and

authenticating said dynamic prompt table file upon loading of the dynamic prompt table file into the terminal.

7. (Original) A method as claimed in claim 6, wherein said authenticating step comprises the step of digitally signing the prompt table file using a private key, and appending to the signed prompt table file a corresponding public key certificate containing information necessary to authenticate the prompt table file.

8. (Original) A system as claimed in claim 7, further comprising the steps of storing said private key on a smartcard and only permitting a secure processor embedded in the smartcard to access the private key.

9. (Original) A system as claimed in claim 8, wherein all digital signing operations requiring access to said private key are carried out by said secure processor.

10. (Original) A system as claimed in claim 7, wherein said smartcard further has stored thereon a signer certificate for authenticating said digital signature, said signer certificate being authenticated by a sponsor certificate pre-installed in the terminal.